



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/699,165	10/31/2003	Jonathan D. Herbach	07844-623001	1607
21876	7590	09/20/2007	EXAMINER	
FISH & RICHARDSON P.C. P.O. Box 1022 MINNEAPOLIS, MN 55440-1022			DUNN, DARRIN D	
ART UNIT		PAPER NUMBER		
2121				
MAIL DATE		DELIVERY MODE		
09/20/2007		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)
	10/699,165	HERBACH ET AL.
	Examiner Darrin Dunn	Art Unit 2121

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 31 October 2003.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-34 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-34 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on 31 October 2003 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO/SB/08)
 Paper No(s)/Mail Date 10/31/2003.

4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____.
 5) Notice of Informal Patent Application
 6) Other: _____.

DETAILED ACTION

1. This Office Action is responsive to the communication filed on 10/31/2003.
2. Claims 1-34 have been presented for examination.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-6, 8-9, 12-20, 23-29, and 33 are rejected under 35 U.S.C. 102(e) as being anticipated by Raley et al. (USPN 20030196121).

5. As per claims 1,12 and 23, RALEY ET AL. teaches a method comprising:
receiving, at a server, - 120 [FIG 1] a request from a client – 130 to take an action with respect to an electronic document – [0045 lines 1-2];
obtaining, at the server and in response to the request, a software program - security module [0064 lines 3-10] comprising instructions operable to cause one or more data processing apparatus to perform operations effecting an authentication procedure – enforcing usage rights [0064 line 11]; and
sending the authentication program – loading requisite components in response to client computer [0064 lines 3-10] to the client for use in identifying a current user and

controlling the action with respect to the electronic document – usage rights [0065 lines 14-19]

based on the current user and document-permissions information associated with the electronic document.

6. As per claims 2,13, and 24 RALEY ET AL. teaches the method of claim 1, wherein obtaining the software program comprises requesting and receiving the software program from a second server – 220' FIG 2 .

7. As per claims 3 and 14, RALEY ET AL. teaches the method of claim 1, further comprising:

receiving an updated authentication procedure – [0092 lines 7-11 e.g., updated security manager] ;

receiving a subsequent request from the client to take the action with respect to the electronic document – [0092 lines 3-5] ;

obtaining, in response to the subsequent request, a new software program –updated security manager [0092 lines 7-11] comprising instructions operable to cause one or more data processing apparatus to perform operations effecting the updated authentication procedure [0092]; and

sending the new software program to the client –1410 [FIG 14] for use in identifying the current user and controlling the action with respect to the electronic document based on the current user and the document-permissions information associated with the electronic document (security module provides for usage rights with regard to electronic document).

8. As per claims 4 and 15, RALEY ET AL. teaches the method of claim 1, wherein the software program uses an existing interface – 236 [FIG 2] provided by the client to communicate authentication information to the server lines

9. As per claims 5 and 16, RALEY ET AL. teaches the method claim 1, further comprising: receiving credentials information - signature [0068 lines 8-11] from the client derived at least in part based on input obtained by the client using the software program; and communicating with a third party authentication server to authenticate the current user based on the credentials information – [0089].

10. As per claims 6 and 17, RALEY ET AL. teaches the method of claim 5, wherein the input obtained by the client comprises text input –message [0068 line 8]

11. As per claims 8 and 19, RALEY ET AL. teaches the method of claim 1, further comprising:

receiving from the client an authentication receipt obtained by the client – recording charge back [0082 lines 3-6] from a third party authentication server - 160 based on input obtained by the client using the software program; and verifying the current user – user information on file [0083] with the third party authentication server using the authentication receipt.

12. As per claims 9 and 20, RALEY ET AL. teaches the method of claim 1, further comprising:

retrieving a document identifier – [0066 lines 4-6] from the request; determining whether user authentication is needed based on the document identifier and the action – use restrictions [0066 line 6] ;

sending information specifying an acceptable authentication procedure – [0066 lines 11-14]; and

receiving an authentication procedure update request from the client – [0066 lines 16-18].

13. As per claim 25, RALEY ET AL. teaches the system of claim 23, wherein the client includes a security handler –security module [0088] that provides a server-communication interface to the software program.

14. As per claim 26, RALEY ET AL. teaches the system of claim 23, further comprising a third party authentication server – trusted server [0092 line 9] that authenticates the current user based on credentials information derived at least in part based on input obtained at the client using the software program.

15. As per claim 27, RALEY ET AL. teaches the system of claim 26, wherein the client obtains an authentication receipt –certified program [0092] from the third party authentication server and forwards the authentication receipt to a server for verification.

16. As per claim 28, RALEY ET AL. teaches the system of claim 23, wherein the server comprises:

a server core –220 [FIG2] with configuration and logging components –225 [FIG 2];
an internal services component – 226 that provides functionality across dynamically loaded methods; and

dynamically loaded external service providers -224, including an authentication service provider.

17. As per claim 29, RALEY ET AL. teaches the system of claim 23, further comprising:
a business logic tier - [0072 lines 1-3] comprising a cluster of document control servers,

including the server;

an application tier including the client comprising a viewer client, a securing client, and an administration client – 230 [FIG 2 e.g., browser, i.e., viewing client, securing client, i.e. security module, administration client, i.e., connection module]; and

a load balancer 220]0095 lines 1-5] that routes client requests to the document control servers.

18. As per claim 33, RALEY ET AL. teaches a system comprising:

server means for dynamically obtaining and sending authentication processes in response to client requests to take actions with respect to electronic documents – [0064]; and client means [0061] for interfacing with a received authentication process to identify a current user and for controlling actions with respect to electronic documents based on the current user and document-permissions information.

Claim Rejections - 35 USC § 103

19. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

20. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

Art Unit: 2121

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

21. Claims 7 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Raley et al. (USPN 20030196121) in view over Leah et al. (USPN 6986039).

22. As per claim 7 and 18, Raley et al. does not disclose the limitation if implementing biometrics as input obtained by a client. Leah et al. teaches identifying a user via biometric information [COL 1 lines 55-57].

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to utilize biometrics as a form of user identification when used for credential verification. Raley et al. provides a means for users to access protected documents, and further provides a secures means to do so. In effect, since biometrics provide an additional secured means of accessing protected content, it would have been obvious to utilize biometrics when accessing protected content.

23. Claims 10-11 and 21-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Raley et al. (USPN 20030196121) in view over Pensak et al. (USPN 6449721).

24. As per claims 10-11 and 21-22, Raley et al. does not disclose the limitation where access permissions include a level of granularity smaller than the electronic document or a per-page granularity. Pensak et al. teaches breaking a document into segments such that the segments may access different policies, including setting page limitations ([COL 2 lines 25-30]).

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to define a subset of permissions. Since a document may be divided into various

segments, and given that user permission may vary per segment, it would have been obvious to have defined specific authorization policies pertaining to the respective document segments.

25. Claims 30-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Raley et al. (USPN 20030196121) in view over Larose (USPN 20020087876).

26. As per claim 30, Raley does not disclose the limitations of claims 30; however, Larose teaches the system of claim 23, wherein the server comprises a permissions-broker server including a translation component (see page 4 paragraph 59), the local electronic document comprises a document secured previously (versions) by the permissions-broker server, and the translation component being operable to translate first document-permissions information in a first permissions-definition format into second document-permissions information in a second permissions-definition format in response to the request being received from the client (see pages 4-5 paragraphs 59-62 and 67)

Therefore, it would have been obvious to a person skilled in the art to have provided a server operable to store varying versions of an electronic document. Since it is foreseeable that permissions pertaining to electronic documents may change, it would have been necessary to store multiple versions of a document. In addition, Larose states persons having ordinary skill in the this art will readily recognize that the present invention can be incorporated into any number of types and versions of software application.

27. As per claim 31, RALEY ET AL. teaches the system of claim 23, wherein the server comprises a permissions-broker server operable to identify information associated with the local electronic document in response to the request, the associated information being retained at the server and indicating a second electronic document different (first and second version) from and

associated with the local electronic document, the server being operable to relate information concerning the second electronic document to the client to facilitate the action to be taken (see page 3 paragraphs 35-36)

28. Claim 32 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Raley et al. (USPN 20030196121) in view over Larose (USPN 20020087876) and in further view of Non-Patent Literature “PageRecall: The Key to Document Protection, Authentica, Inc., Whitepaper. <http://www.authentica.com/products/white>.”

29. As per claim 32, Raley et al. discloses the limitations of claim 23, but is silent with regard to synchronizing offline access information. Larose substantially discloses a server operable to synchronize offline access information with the client in response to the client request (page 6, paragraph 92), the offline access information comprising a first key associated with a group, the first key being usable at the client to access a distributed document by decrypting a second key (token) in the distributed document, and the client allows access to the distributed document, when offline, by a user as a member of the group, using the first key to decrypt the second key in the distributed document and governing actions with respect to the distributed document and governing actions with respect to the distributed document based on document-permissions associated with the distributed document (page 6, paragraphs 91-92). Although Larose is silent about decryption being performed “offline,” one embodiment discloses that software may be previously installed and access to the document may occur upon client authentication (paragraph 93). Non-Patent Literature discloses that wherein in “work offline mode” uses can access encrypted document offline once the server authenticates the user, and therefore a copy of the key for decryption is sent by the server for the authorized document (see page 6). Therefore, it

would have been obvious to one of ordinary skill in the art at the time the invention was made to allow the document to be accessed offline upon user authentication. In effect, document access may occur exclusive of users being online while retaining the necessary security as suggested by the NPL (page 6)

30. As per claim 34, Larose teaches a server means for transparently providing offline access information for controlled documents to pre-authorize a client to allow actions by a user as a member of a group of users, - (page 6 paragraph 92) the offline access information comprising a first key associated with the group, the first key being useable at the client to access an electronic document by decrypting a second key in the electronic document; and
client means for accessing the electronic document using the offline access information (page 6 paragraphs 91-92).

Conclusion

31. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

20030217264 – system and method for providing a secure environment during the use of electronic documents and data

20030196120 – method and apparatus for automatic deployment of a rendering engine

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Darrin Dunn whose telephone number is (571) 270-1645. The examiner can normally be reached on EST:M-R(8:00-5:00) 9/5/4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Anthony Knight can be reached on (571) 272-3687. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DD
09/10/07



Anthony Knight
Supervisory Patent Examiner
Art Unit 2121